(12) UK Patent Application (19) GB (11) 2 242 295 (13) A

(43) Date of A publication 25.09.1991

(21) Application No 9102940.5

(22) Date of filing 12.02.1991

(30) Priority data
(31) 9003112 (32) 12.02.1990 (33) GB

(51) INT CL[5]
G06F 12/14

(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
EP 0192243 A2 EP 0152900 A2 EP 0006355 A1
US 3893084 A

(58) Field of search
UK CL (Edition K) G4A AAP
INT CL[5] G06F 1/00 12/14

(71) Applicant
International Computers Limited

(Incorporated in the United Kingdom)

ICI House, Putney, London, SW15 1SW,
United Kingdom

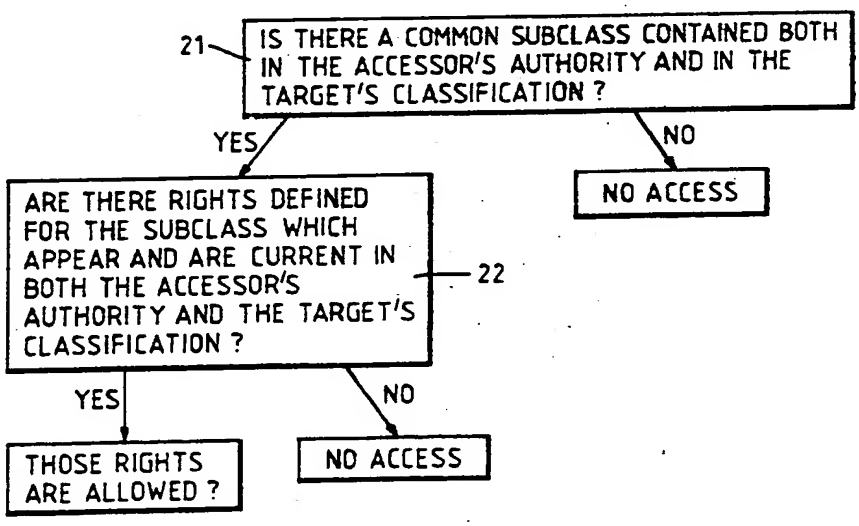
(72) Inventor
Roy William Jones

(74) Agent and/or Address for Service
D C Guyatt
STC Patents, West Road, Harlow, Essex, CM20 2SH,
United Kingdom

(54) **Access control in a data processing system**

(57) In a method of controlling access in a data processing system, firstly a set of attributes is defined for targets that may be accessed and for accessors that may access the targets. A set of access security classes is then defined in terms of these attributes or other classes. Each class has a set of allowable operations associated with it. Each target is assigned a classification comprising one of the classes and a set of allowed operations. Each accessor is assigned an authority consisting of one of the classes and a set of allowed operations. An accessor is allowed to access a target only if there is a common sub-class contained in both the accessor's authority and in the target's classification, 21, and if the required operation is defined for that subclass and appears in both the accessor's authority and in the target's classification, 22.

Fig.2.



At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

GB 2 242 295 A

Fig. 1.

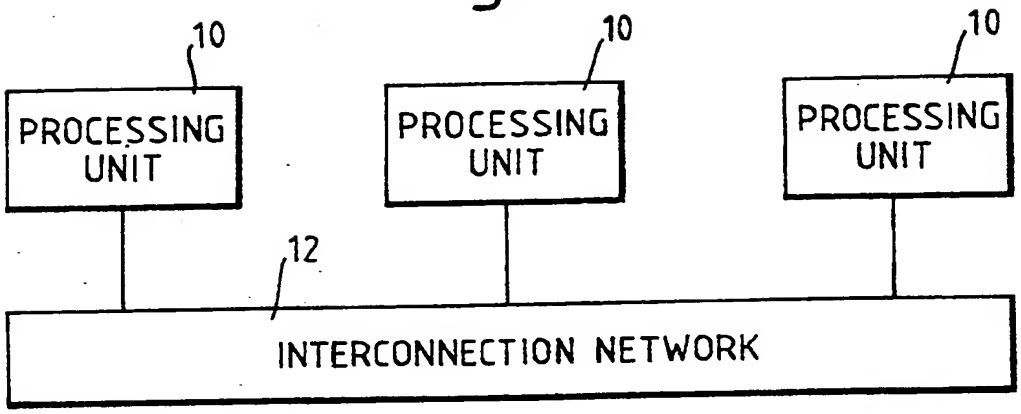

10
10
10
PROCESSING UNIT
PROCESSING UNIT
PROCESSING UNIT
12
INTERCONNECTION NETWORK

Fig. 3.

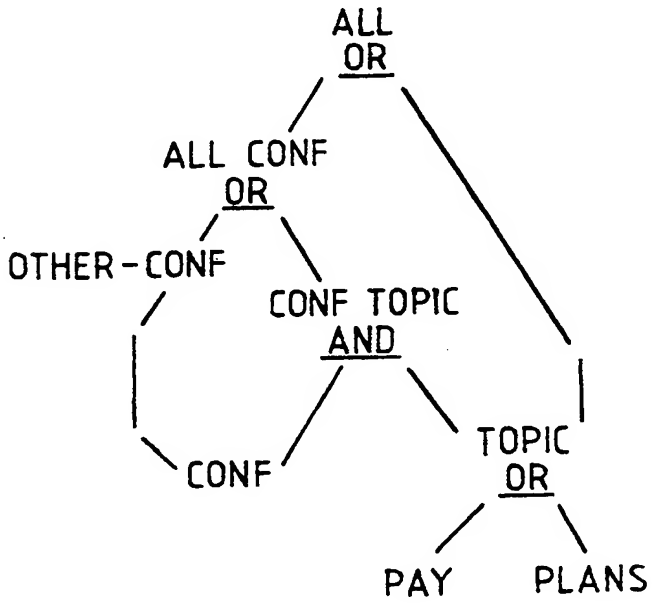
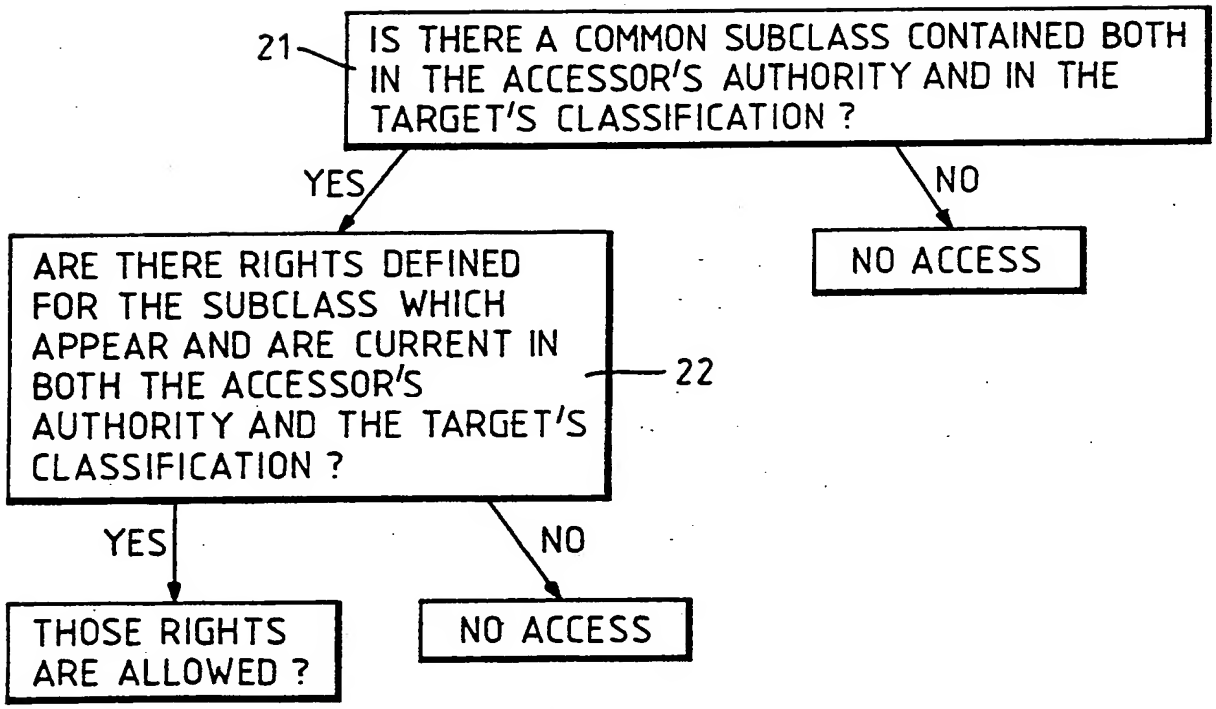

ALL
OR
ALL CONF
OR
OTHER-CONF
CONF TOPIC
AND
CONF
TOPIC
OR
PAY
PLANS

Fig.2.


21
IS THERE A COMMON SUBCLASS CONTAINED BOTH IN THE ACCESSOR'S AUTHORITY AND IN THE TARGET'S CLASSIFICATION ?
YES
NO
NO ACCESS
ARE THERE RIGHTS DEFINED FOR THE SUBCLASS WHICH APPEAR AND ARE CURRENT IN BOTH THE ACCESSOR'S AUTHORITY AND THE TARGET'S CLASSIFICATION ?
22
YES
NO
THOSE RIGHTS ARE ALLOWED ?
NO ACCESS

ACCESS CONTROL MECHANISM

This invention relates to an access control mechanism data processing system.

According to the invention there is provided a method of controlling access in a data processing system, comprising

(a) defining a set of attributes for targets that may be accessed and for accessors that may access the targets,

(b) defining a set of security classes, each security class comprising a combination of said attributes and/or other classes,

(c) associating with each security class a set of operations applicable to that class,

(d) assigning a classification to each target, comprising one of said classes and a set of allowed operations,

(e) assigning an authority to each accessor, comprising one of said classes and a set of allowed operations,

(f) in response to a request by an accessor to perform an operation on one of the targets, permitting the operation only if there is a common subclass contained both in the accessor's authority and in the target's classification, and if the operation is

defined for that subclass and appears both in the accessor's authority and in the target's classification.

One embodiment of the invention will now be described by way of example,with reference to the accompanying drawings, of which:

Figure 1 is a block diagram of a distributed data processing system embodying the invention;

Figure 2 is a flow chart showing the way in which access is controlled; and

Figure 3 is a schematic diagram showing an example of a set of security classes.

Referring to Figure 1, the distributed data processing system comprises a plurality of data processing installations 10, which communicate with each other by way of an interconnection network 12. The data processing installations may be individual workstations, or may be computers with attached workstations. The network may be a local area network, or telecommunications lines, or a combination of both.

The system includes a number of objects to which it is required to control access, these objects being referred to herein as targets. For example, the targets may include data items such as documents or files, stored in the individual data processing installations.

These targets may be accessed by various entities, referred to herein as accessors. For example, an accessor may be a human end user, an individual work station or a software entity within a computer.

The access control mechanism for the system is implemented as follows.

First, a set of attributes is declared for the system. Each attribute is a unique identifier within the set for the system. The attributes are chosen as names for individual characteristics of the system components which are known to be significant to access control. Thus, for example, data items may have the attributes "confidential", "project N", "staff pay" etc., and end users may have the attributes "employee", "manager" etc.

A set of security classes is then defined, each class consisting of a logical combination of one or more of the attributes and/or of other defined classes. Each of these classes may consist of one or more subclasses, where a subclass is defined as the result of deleting zero or more logical OR alternatives from a class, or replacing one or more of its qualifiers by a subclass of the qualifier. (See the definition of a class below).

A set of allowable operations is then assigned to each class and attribute. Typical operations might be, for example "interrogate", "modify" or "summarise".

Each of the targets is assigned a classification consisting of one of the security classes, along with a set of allowable operations, chosen from those of its class.

Similarly, each of the accessors is assigned an authority consisting of one of the security classes, along with a set of allowable operations, chosen from

those of the class. An accessor which may itself be accessed has both a classification and an authority.

The definitions of the classes, the authorities, and the classifications are all stored in a database in the system, so that they can be accessed by the access control mechanism.

Referring now to Figure 2, when a particular accessor requires to access a particular target to perform a specified operation, the operation of the access control mechanism is as follows:

First, the access control mechanism checks (21) whether there is a common subclass contained both in the accessor's authority and in the target's classification. If not, then no access is permitted.

If, however, there is a common subclass, the access control mechanism now checks (22) whether there are any operations defined for this common subclass which appear both in the accessor's authority and in the target's classification. If not, then again no access is permitted.

If there are such operations, then the accessor is allowed to perform those, but no others, on the target. The operation required is, therefore, allowed if it is one of these.

The form of a security class may be expressed as follows, using an extended Backus-Naur notation:

```
class-definition ::= class-name, ':', definition-list, ';';
definition-list  ::= and-list  |  or-list;
and-list         ::= qualifier, [and qualifier];
or-list          ::= qualifier, [or qualifier];
qualifier        ::= attribute  |  class-name;
```

An and-list allows the expression of a list of qualifiers which must always be present in an instance of the class defined. An or-list allows the expression of a list of qualifiers one or more of which must be present in an instance of the class defined. Other forms of expression could be provided such as, for example, to specify the combination "any N of", or "exclusive OR". They could then be used to allow more concise class definitions and be represented in the access control mechanism for greater efficiency. A qualifier is defined as an attribute or a class-name so that a class may be expressed in terms of other classes.

As an example, consider a system in which documents are stored electronically and in which access to the documents is to be controlled according to the trustworthiness and position of the accessors. The documents are classified using the attributes "confidential", "pay" and "plans". Some documents about pay are confidential, some are not. Some documents about plans are confidential, some are not. Some documents are confidential but are not concerned with either pay or plans.

In this example, the following security classes may be defined:

(i) all: all-conf or topic;
(ii) all-conf: other-conf or conf-topic;
(iii) other-conf: conf;
(iv) conf-topic: conf and topic;
(v) topic: pay or plans;

Figure 3 shows these classes schematically.

A set of operations is defined for each of these classes. For example, the class "all" may have the operation "interrogate" and "modify" associated with it,

while the class "topic" may have the operation "summarise" associated with it.

Each document held in the system has one of these classes assigned to it as its security classification, along with a set of allowed operations. For example, one particular document may be assigned the classification "conf-topic".

Similarly, each accessor of the system is assigned one of the classes as an authority along with a set of allowed operations. For example, a particular grade of employee may have the authority "topic".

It will be seen that this employee would not be allowed to access documents with the classification "conf-topic" since conf-topic and topic do not have any common sub-class. (Topic is not a subclass of conf-topic since conf-topic consists of an AND combination, rather than an OR). However, this employee would be allowed to access documents with classification "topic", to perform operations which appear both in the employee's authority and the documents classification.

By way of example, the following format may be used for representing the security classes, and storing them in the system. These format definitions refer to "rights" rather than operations. A right is a collection of operations to all of which the same access control rules apply. Thus "right" may be substituted for "operation" in the previous description.

class name(12 bits): an identifier chosen to be unique for the system within which access is controlled.

class designator(4 bits): value 0000 signifies an OR list; i.e. combination of qualifiers may appear in an instance of this class,

value 0001 signifies an AND list; i.e. all qualifiers must appear in an instance of this class,

other values reserved for possible use.

authority(16 bits): this is a pointer to the definition of an authority (which is a security class with rights and therefore has this same format); a value of sixteen zeros indicates that no authority is associated with the class.

number of qualifiers(8 bits): an unsigned binary number indicating the number of qualifiers which follow.

qualifier: this may occur one or more times as indicated by "number of qualifiers". Each occurrence has the following format:

kind of qualifier (1 bit):

value 0 means class,

value 1 means attribute.

qualifier value (15 bits)

If "kind of qualifier" has the value 0 this is a pointer to another class; if "kind of qualifier" has the value 1 this is a binary string representing an attribute.

rights pointer(15 bits): a pointer to the list of rights which apply to the class.

A list of rights has the following format:

number of rights(8 bits): an unsigned binary number indicating the number of rights which follow.

right: this may occur one or more times as indicated by number of rights. Each occurrence has the following format:

right name(16 bits): a binary string representing a right of the class.

list of operations(16 bits): a pointer to a list of operations made available to the possessor of the right.

For example, the above-mentioned "all : all-conf or topic;" would be represented as follows:-

5. A data processing system, comprising

(a) means for storing a set of access classes, each access class comprising a combination of attributes for targets that may be accessed and for accessors that may access the targets, each access class having associated with it a set of operations applicable to that class,

(b) means for storing a classification for each target, the classification comprising one of said classes and a set of allowed operations,

(c) means for storing a clearance for each accessor, the clearance comprising one of said classes and a set of allowed operations, and

(d) means operable in response to a request by an accessor to perform an operation on one of the targets for permitting the operation only if there is a common subclass contained both in the accessor's clearance and in the target's classification, and if the operation is defined for that subclass and appears both in the accessor's clearance and in the target's classification.

6. A data processing system having an access control mechanism substantially as hereinbefore described with reference to the accompanying drawings.

Published 1991 at The Patent Office, Concept House, Cardiff Road, Newport, Gwent NP9 1RH. Further copies may be obtained from Sales Branch, Unit 6, Nine Mile Point, Cwmfelinfach, Cross Keys, Newport, NP1 7HZ. Printed by Multiplex techniques ltd, St Mary Cray, Kent.